IN THE CLAIMS

Please amend Claims 1, 18, 26, 29, and 38 as indicated below. Note that Claim 38 is converted to an independent claim.

1. (currently amended)

A computer implemented method embodied in data structures stored in a computer-readable medium to execute the following steps:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning,

with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence;

generating a signal having a distinct characteristic using the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.

18. (currently amended)

The method of claim 17, wherein halving further comprises executing a single field multiplication per halving operation.

26. (currently amended)

An apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information;

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic;

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic;

the system further configured to execute an elliptic curve method for generating the distinct characteristic; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning, with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence.

29. (currently amended)

An article of manufacture comprising a computer-readable medium storing operational data and executable data structures executable on a processor, the executable data structures comprising:

an encryption engine for operating on distinct characteristics configured to encrypt substantive content representing information;

the encryption engine, further comprising a distinct characteristic generation module for operating on the distinct characteristics;

the distinct characteristic generation module, further comprising an elliptic curve module for providing the distinct characteristics; and

the elliptic curve module, further comprising a point modification algorithm for calculating points related to the distinct characteristic,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning,

with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence.

38. (currently amended)

A computer implemented method embodied in data structures

stored in a computer-readable medium to execute the following

steps:

selecting an elliptic curve method,

~~The method of claim 1,~~ wherein the elliptic curve is over a finite field and the finite field is represented as a field

~~tower.~~ tower;

executing a point modification algorithm to manipulate points

of the elliptic curve method,

wherein the point modification algorithm includes at least

one occurrence of point fractioning;

generating a signal having a distinct characteristic using

the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct

characteristic.

A complete list of all the claims, numbered 1-59, is provided below:

1. (currently amended)

A computer implemented method embodied in data structures stored in a computer-readable medium to execute the following steps:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning,

with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence;

generating a signal having a distinct characteristic using the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.

2. (original)

The method of claim 1, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

3. (original)

The method of claim 1, wherein manipulating the substantive content comprises encrypting the substantive content.

4. (original)

The method of claim 1, wherein manipulating the substantive content comprises decrypting the substantive content.

5. (original)

The method of claim 1, wherein the distinct characteristic is selected from a key and a signature.

6. (original)

The method of claim 2, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

7. (original)

The method of claim 2, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

8. (original)

The method of claim 1, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

9. (original)

The method of claim 2, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

10. (original)

The method of claim 9, wherein the selected property is a membership condition placing the first point in a subgroup.

11. (original)

The method of claim 10, further comprising repeating the point modification algorithm with a second point selected by another entity selected from a deterministic process, a random process, and a third party.

12. (original)

The method of claim 11, wherein the second point is communicated to the point modification algorithm in a format selected from a message and a certificate.

13. (original)

The method of claim 2, further comprising selecting a first point and pre-modifying the first point by a modification operation configured to compensate for some of the processing steps, added and corresponding to execution of a series of steps in accordance with the method.

14. (original)

The method of claim 1, further comprising sending by a sender and receiving by a receiver the substantive content, and wherein the sender executes a first operation during modification for encryption and the receiver executes a second and distinct operation during modification for decryption.

15. (original)

The method of claim 1, wherein generating the distinct characteristic further comprises creating a distinct characteristic selected from a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, and an authentication.

16. (original)

The method of claim 1, further comprising selecting a point and wherein the point is of a type selected from a hyperelliptic curve, an algebraic curve, and abelian variety.

17. (original)

The method of claim 1, wherein modifying a point further comprises halving a point represented in a cartesian space and a point existing in a mapped cartesian space having a cartesian representation.

18. (currently amended)

The method of claim 17, wherein halving further comprises executing a single field multiplication per halving operation.

19. (original)

The method of claim 18, further comprising selecting a point characterized by a cartesian tuple and completing halving using no more than two field multiplications.

20. (original)

The method of claim 19, wherein halving further comprises negative halving including computation of a minus one-half multiple.

21. (original)

The method of claim 1, further comprising computing a fractional multiple of a point selected from a proper fraction, an improper fraction, and a complex fractional multiple.

22. (original)

The method of claim 18, further comprising determining a selection of points to execute a halving operation with respect to, based on testing for membership in a subgroup.

23. (original)

The method of claim 22, wherein testing further comprises reliance on a bit mask of coordinates corresponding to points in the subgroup.

24. (original)

The method of claim 23, wherein testing is executed by testing whether a halving procedure can be executed an arbitrary number of times selected by a user.

25. (original)

The method of claim 24, further comprising determining which of a selected number of points is to be used.

26. (currently amended)

An apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information;

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic;

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic;

the system further configured to execute an elliptic curve method for generating the distinct characteristic; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning, with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence.

27. (original)

The apparatus of claim 26, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

28. (original)

The apparatus of claim 26, wherein the distinct characteristic is configured to be processable by the system for divulging independently to two independent parties a secret to be shared by the two independent parties.

29. (currently amended)

An article of manufacture comprising a computer-readable medium storing operational data and executable data structures executable on a processor, the executable data structures comprising:

an encryption engine for operating on distinct characteristics configured to encrypt substantive content representing information;

the encryption engine, further comprising a distinct characteristic generation module for operating on the distinct characteristics;

the distinct characteristic generation module, further comprising an elliptic curve module for providing the distinct characteristics; and

the elliptic curve module, further comprising a point modification algorithm for calculating points related to the distinct characteristic,

wherein the point modification algorithm includes at least ~~one occurrence~~ five occurrences of point fractioning,

with the inputs to said at least five occurrences after the first depending directly or indirectly on results from the previous occurrence.

30. (original)
The article of claim 29, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

31. (original)
The article of claim 30, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

32. (original)
The article of claim 30, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

33. (original)
The article of claim 29, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

34. (original)
The article of claim 30, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

35. (original)

The article of claim 29, wherein the distinct characteristics are selected from a key and a signature.

36. (previously presented)

The method of claim 1, wherein the elliptic curve is over a finite field;

the finite field is represented by a field polynomial; and

the field polynomial is of low hamming weight.

37. (previously presented)

The method of claim 36, wherein the field polynomial is selected from a binomial, a trinomial, and a pentanomial.

38. (currently amended)

A computer implemented method embodied in data structures

stored in a computer-readable medium to execute the following

steps:

selecting an elliptic curve method,

~~The method of claim 1,~~ wherein the elliptic curve is over a finite field and the finite field is represented as a field ~~tower.~~ tower;

executing a point modification algorithm to manipulate points

of the elliptic curve method,

wherein the point modification algorithm includes at least

one occurrence of point fractioning;

generating a signal having a distinct characteristic using

the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct

characteristic.

39. (previously presented)
The method of claim 38, wherein the field tower comprises an outer field; and
the extension degree of the outer field is selected from the numbers 2,3,5, a product of the numbers, or repeated uses of any of the numbers.

40. (previously presented)
The method of claim 38, wherein the field tower has more than two levels.

41. (previously presented)
The method of claim 38, wherein the field tower comprises an inner field, having arithmetic, and wherein the arithmetic is accelerated by using pre-computed tables for operations selected from the group consisting of multiplication, squaring, taking the square root, division, reciprocation, taking the logarithm, exponentiation, calculating solutions of quadratic equations, and calculating the solutions of polynomial equations.

42. (previously presented)
The method of claim 1, wherein the point modification algorithm comprises solving a quadratic equation using an efficient algorithm.

43. (previously presented)
The method of claim 1, wherein the point modification algorithm comprises computing a reciprocal of a field element using an efficient algorithm.

44. (previously presented)
The method of claim 1, wherein the point modification algorithm comprises at least one of adding and subtracting of elliptic curve points using an efficient algorithm.

45. (previously presented)
The method of claim 44, wherein the addition and subtraction comprises computing a reciprocal of a field element using an efficient algorithm.

46. (previously presented)
The method of claim 1, wherein the point modification algorithm comprises point multiplication using a sliding-window method.

47. (previously presented)
The method of claim 1, wherein the point modification algorithm comprises at least two occurrences of point fractioning chained together.

48. (previously presented)
The method of claim 47, wherein the elliptic curve points comprise intermediate points, having coordinates, and wherein the computation of some of the coordinates is omitted.

49. (previously presented)
The method of claim 1, wherein the point modification algorithm further comprises choosing a multiplier having a low hamming weight.

50. (previously presented)
The method of claim 1, wherein the point modification algorithm includes point addition and subtraction steps and the point modification algorithm is chosen to minimize the number of steps.

51. (previously presented)
The method of claim 1, wherein the point modification algorithm is an addition-subtraction chain, intermixed with point fractioning.

52. (previously presented)
The method of claim 1, wherein the elliptic curve is over a finite field, and the size of the finite field is increased such that a smaller number of addition and subtraction steps may be combined with a larger number of point fractioning steps, such that the overall computation effort is reduced, while preserving a specified level of security.

53. (previously presented)
The method of claim 42, wherein the efficient algorithm is accelerated by using a Half-Trace formula.

54. (previously presented)
The method of claim 42, wherein the efficient algorithm is accelerated by using the relationship between Qsolve(C) and Qsolve(C^2).

55. (previously presented)
The method of claim 42, wherein the required storage of the efficient algorithm is reduced by using the relationship between Qsolve(C) and Qsolve(C^2).

56. (previously presented)

The method of claim 1, wherein the point modification algorithm further comprises:

using a plurality of representations of the points;

using input points in one or more representations to produce output points in a different representation;

selecting representations that are optimal for succeeding point modification algorithms; and

wherein at least three changes of representation occur.

57. (previously presented)

The method of claim 1, wherein at least some of the points are represented in XR representation.

58. (previously presented)

The method of claim 56, further comprising switching between the XR and XY representations.

59. (previously presented)

A computer implemented method embodied in data structures stored in a computer-readable medium to execute the following steps:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method, the point modification algorithm comprising one or more ambiguous point triplication steps, where the ambiguity is resolved by determining whether a point is twice halvable;

generating a signal having a distinct characteristic using the elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.